4/2022
73 – 96

Rechtsprechung
„Ibiza-Video" zulässig
V. Haidinger/M. Löffler

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Richtig pfeifen – Umsetzung der Whistleblowing-RL

Wir haben Dinge erfahren, die uns sonst wohl nicht zur Kenntnis gebracht worden wären

Interview mit Maximilian Wellner, Greiner AG

Datenschutzkonforme Umsetzung von Hinweisgebersystemen

Stefan Niederstrasser und Sebastian Kneidinger

Datenschutzrechtliche Aspekte zum HinweisgeberInnenschutzG

Dietmar Mühlböck

FAQ: Worauf bei Logdateien von Hinweisgebersystemen achten?

Michael Löffler

Und täglich grüßt das Auskunftsrecht

Theresia Leitinger

Ablauf des Prüfverfahrens vor der DSB

Andreas Zavadil und Andreas Rohner

Checkliste Betriebsrat und Datenschutz

Hans-Jürgen Pollirer

ISSN 2313-5409

dako.manz.at

MANZ

Österreichische Post AG PZ 18Z041356 P Verlag Manz, Gutheil Schoder Gasse 17, 1230 Wien

Stefan Niederstrasser/Sebastian Kneidinger
KPMG Law/KPMG Austria

Datenschutzkonforme Umsetzung von Hinweisgebersystemen

Vertraulichkeit; Offenlegung; Identität des Hinweisgebers; Dokumentationspflichten; Betroffenenrechte. Whistleblower helfen bei der Aufdeckung von Rechtsverstößen, gleichzeitig müssen sie vor Repressalien geschützt werden. Bei der Implementierung von Hinweisgebersystemen sind datenschutzrechtliche Aspekte zu beachten.

Hinweisgeber (auch „Whistleblower") liefern einen wichtigen Beitrag zur (frühzeitigen) Aufdeckung von Rechtsverstößen. Das österr HinweisgeberInnenschutzgesetz **(HSchG)** – als Umsetzung der „Whistleblower-Richtlinie" (EU) 2019/1937 **(WB-RL)** – wird künftig umfassende Schutzbestimmungen für Hinweisgeber*innen vorsehen. Zur Erleichterung solcher Meldungen werden auf nationaler Ebene „externe" Meldekanäle implementiert und Unternehmen und juristische Personen des öffentlichen Rechts verpflichtet, organisationsinterne Hinweisgebersysteme einzurichten. Letzteres ist von Organisationen mit mehr als 249 Beschäftigten binnen sechs Monaten nach Inkrafttreten des Gesetzes und von Organisationen mit 50–249 Beschäftigten bis 18. 12. 2023 umzusetzen.

Der Entwurf des HSchG vom 3. 6. 2022 war bis zum 15. 7. 2022 in Begutachtung. Österreich befindet sich – wie viele andere EU-Staaten – mit der Umsetzung der WB-RL in Verzug. **Dieser Artikel bezieht sich nur auf den Stand dieses Gesetzesentwurfs.**

Angesichts der mit der Einführung eines Hinweisgebersystems verbundenen technischen, organisatorischen und rechtlichen Herausforderungen empfiehlt es sich, bereits jetzt erste Schritte zur Vorbereitung zu setzen. Zu beachten ist dabei insb, dass das HSchG nur die Meldung von Verstößen gegen gewisse Vorschriften regelt (§ 3 HSchG). Die Meldung von Verstößen gegen andere Vorschriften fällt nicht unter den sachlichen Geltungsbereich des HSchG, weshalb dies auch nicht nach den datenschutzrechtlichen Sonderregelungen des HSchG, sondern nach allgemeinem Datenschutzrecht zu beurteilen ist.

Im Folgenden findet sich ein Überblick zu den wichtigsten Herausforderungen und Lösungswegen aus Sicht des Datenschutzrechts.[1] Der Fokus liegt auf den verpflichtenden Hinweisgebersystemen gem HSchG. Abschließend werden unter Punkt 8. noch datenschutzrechtliche Fragen iZm „freiwilligen" Hinweisgebersystemen behandelt.

1. Rechtsgrundlagen und Verantwortlichkeiten

Als wesentlichstes Grundprinzip der DSGVO gilt, dass jede Datenverarbeitung einer entsprechenden Rechtsgrundlage bedarf.[2] Im HSchG werden die Ermächtigungen zur Datenverarbeitung sowie auch die ex lege-Verantwortlichkeiten primär im § 8 HSchG geregelt.

Die Zulässigkeit der Verarbeitung „normaler" personenbezogener Daten iZm Hinweisgebersystemen ergibt sich aus § 8 Abs 1, 2 HSchG iVm Art 6 Abs 1 lit c, e DSGVO, vorausgesetzt die Verarbeitung

- ist für die Zwecke gem §§ 1, 8 Abs 2 Z 1 HSchG erforderlich **(Grundsatz der Zweckbindung)** und
- wird auf Daten eingeschränkt, die *„zur Feststellung und Ahndung einer Rechtsverletzung benötigt werden"* **(Grundsatz der Datenminimierung)**.

Dies gilt jedoch nur für die Verarbeitung personenbezogener Daten von Hinweisgeber*innen, von Personen, die von der Hinweisgebung betroffen sind, und von Personen, die von Folgemaßnahmen betroffen oder in Folgemaßnahmen involviert sind.

Diese Ermächtigung zur Datenverarbeitung gilt für die folgenden Personen/Stellen/Behörden, die **ex lege als Verantwortliche iSv Art 4 Z 7 DSGVO gelten** (§ 8 Abs 2 HSchG):

- Hinweisgeber*innen (die Qualifikation von Hinweisgeber*innen als Verantwortliche wurde in Stellungnahmen im Begutachtungsverfahren stark kritisiert[3])
- interne[4] und externe Stellen,
- die Leitung eines Unternehmens (in den Fällen des § 13 Abs 2 HSchG), und
- Behörden, die um Austausch oder Übermittlung personenbezogener Daten ersucht sind.

Außerdem sind Unternehmen und juristische **Personen des öffentlichen Rechts**[5] gem § 8 Abs 6 iVm § 11 Abs 1 HSchG ermächtigt, Hinweisgebersysteme einzurichten, und gelten für die Einrichtung dieser Systeme als Verantwortliche iSv Art 4 Z 7 DSGVO.

Die Ermächtigung gem § 8 Abs 2 HSchG gilt zudem auch für die Verarbeitung von personenbezogenen **Daten gem Art 10 DSGVO**; wird aber insofern eingeschränkt, als dies nur *„im Fall unbedingter Erforderlichkeit erfolgen"* darf und schriftlich zu dokumentieren ist (§ 8 Abs 4 HSchG). Enthält ein Hinweis einen plausiblen und begründeten Verdacht eines strafrechtlich oder verwaltungsstrafrechtlich relevanten Verhaltens, wird die Verarbeitung dieser Daten gem Art 10 DSGVO wohl so lange *„unbedingt erforderlich"* sein, wie die rasche Prüfung der Stichhaltigkeit des Hinweises andauert, und darüber hinaus bis zur rechtskräftigen Entscheidung in allfälligen verwaltungsstrafrechtlichen oder gerichtlichen Verfahren.[6]

Für die Verarbeitung personenbezogener **Daten gem Art 9 Abs 1 DSGVO** sieht § 8 Abs 3 HSchG eine besondere Ermächtigung vor, die unter folgenden Voraussetzungen steht:

- **Unbedingte Erforderlichkeit** für die Erreichung der Zwecke gem §§ 1, 8 Abs 2 Z 1 HSchG;

[1] Siehe auch *Brunner/Nagel*, Whistleblowing – Sicherstellung des Hinweisgeberschutzes im Lichte der DSGVO, Dako 2020/21; *Pollirer*, Checkliste Whistleblowing, Dako 2020/23; sowie aus arbeitsrechtlicher Sicht *Stella/Winter*, Whistleblowing-RL: Ungelöste Rechtsfragen für die betriebliche Umsetzung, ZAS 2021/22. [2] Art 5 Abs 1 lit a iVm Art 6 Abs 1 DSGVO. [3] Vgl Stellungnahme Transparency International Austria, https://ti-austria.at/wp-content/uploads/2022/07/TI-Austria-Stellungnahme-zum-Entwurf-fuer-das-HSchG_Juli-2022.pdf. Anzumerken ist, dass der nationale Gesetzgeber damit konfrontiert ist, dass die DSGVO keinen Regelungsspielraum für die Einschränkung von Verpflichtungen bestimmter Verantwortlicher vorsieht. [4] Der Österreichische Rechtsanwaltskammertag moniert in seiner Stellungnahme, dass interne Stellen teilweise keine rechtsfähigen Abteilungen sein werden und folglich wohl das jeweilige Unternehmen selbst als Verantwortlicher zu qualifizieren wäre; vgl Seite 8 www.parlament.gv.at/PtWeb/api/s3serv/file/236d23dc-feff-467f-b68e-f59bfa0c9c67. [5] Vgl die Legaldefinition von „juristische Person des öffentlichen Rechts" in § 5 Z 6 HSchG. [6] Vgl Art. 29-Gruppe, Stellungnahme 1/2006, WP 117, 14.

- **erhebliches öffentliches Interesse** an der Verarbeitung zur Erreichung dieser Zwecke und
- **Einsatz wirksamer Schutzmaßnahmen** für die Rechte und Freiheiten der betroffenen Personen.

Durch die zit Bestimmungen des § 8 HSchG werden – nach Ansicht der DSB – die (vorstehend aufgezählten) *„zuständigen Stellen gem Art 6 Abs 1 lit c und e, Art 9 Abs 2 lit g und Art 10 DSGVO bzw §§ 38 und 39 DSG ermächtigt […], die erforderlichen personenbezogenen Daten für Zwecke des HSchG im erforderlichen Ausmaß zu verarbeiten“*.[7]

2. Vertraulichkeit der Identität des Hinweisgebers

Interne Stellen sind verpflichtet, die Identität von Hinweisgeber*innen (sowie alle anderen Informationen, aus denen die Identität direkt oder indirekt abgeleitet werden kann) geheim zu halten (§ 7 Abs 1 HSchG). Dies gilt gem § 13 Abs 3 HSchG auch gegenüber der *„Leitung des Unternehmens“* (dies sind insb die vertretungsbefugten Personen und *„verantwortlichen Beauftragten“* iSv § 9 Abs 1 VStG[8]). IdS sieht § 12 Abs 1 HSchG zudem vor, dass Hinweisgebersysteme *„so sicher zu planen, einzurichten und zu betreiben [sind], dass die Vertraulichkeit der Identität der Hinweisgeberin oder des Hinweisgebers und Dritter, die in der Meldung erwähnt werden, gewahrt bleibt.“*

Zur Erfüllung dieser Verpflichtungen – sowie aller weiterer Vorgaben zum rechtskonformen Verfahren iZm Hinweisen iSd HSchG[9] – müssen (datenschutzrechtlich ohnehin verpflichtende) geeignete technische und organisatorische Maßnahmen (Art 32 DSGVO) sowie **Maßnahmen** iSv data protection by design and default (Art 25 DSGVO) getroffen werden, wie etwa:

- Erstellung/Umsetzung eines entsprechenden Berechtigungskonzepts für das verwendete Hinweisgebersystem;
- Festlegung verbindlicher Abläufe für die interne Stelle inklusive entsprechender Schulungen (jedoch ohne dadurch die gem § 12 Abs 2 HSchG gebotene Unabhängigkeit zu gefährden);
- eine dem Stand der Technik entsprechende Verschlüsselung[10]; und
- Implementierung einer durchgehenden Protokollierung (Log-Files) der Zugriffe und Änderungen im Hinweisgebersystem und sichere Verwahrung dieser Informationen.

Für den Fall, dass der Hinweis anderen Beschäftigten (als denen der internen Stelle) bekannt wird, trifft diese unmittelbar die Verschwiegenheitsverpflichtung nach § 7 Abs 2 HSchG. Demnach sind Inhalt des Hinweises sowie Identität der Hinweisgeber*innen geheim zu halten, abgesehen von der gebotenen Weiterleitung an die interne Stelle.

PRAXISTIPP

Es empfiehlt sich, die Beschäftigten – unter Hinweis auf potenzielle Folgen – möglichst klar auf diese Verpflichtung hinzuweisen: Verletzungen der Vertraulichkeitsbestimmungen der §§ 7, 13 Abs 3 HSchG können zu Verwaltungsstrafen bis zu € 20.000,– führen.

Außerdem kann die Offenlegung der Identität von Hinweisgeber*innen oder von in Meldungen erwähnten Personen einen **Datenschutzvorfall** iSv Art 4 Z 12 DSGVO verwirklichen. Diesfalls ist zu prüfen (und entsprechend zu dokumentieren), ob eine Meldung an die DSB (Art 33 DSGVO) oder auch eine Information der betroffenen Personen (Art 34 DSGVO) erforderlich ist.

3. Offenlegung der Identität des Hinweisgebers bei Zustimmung?

Nach dem Wortlaut der WB-RL wäre die Offenlegung der Identität gegenüber anderen als den zuständigen Personen der internen Stelle bei ausdrücklicher Zustimmung der Hinweisgeber*innen zulässig.[11] Dies wird in der Praxis va dann von Interesse sein, wenn sich Hinweisgeber*innen Vorteile aus der Offenlegung ihrer Identität gegenüber der Leitung des Unternehmens erwarten. Das HSchG enthält diesbezüglich keine Regelung. Vielmehr sieht § 13 Abs 3 HSchG für interne Stellen ein ausnahmsloses Verbot vor, die Identität von Hinweisgeber*innen gegenüber der Leitung des Unternehmens offenzulegen.

PRAXISTIPP

Sollten Hinweisgeber*innen eine Offenlegung ihrer Identität wünschen, ist internen Stellen zu raten, die Hinweisgeber*innen – nach Aufklärung über potenzielle Risiken – um selbstständige Offenlegung zu ersuchen.

4. Externe Dienstleister und Kooperationen

Viele Organisationen ziehen zur technischen Implementierung des Hinweisgebersystems externe Dienstleister heran. Dabei ist zu beachten, dass hier im Standardfall eine Auftragsverarbeitung iSv Art 28 DSGVO vorliegt und ein **Auftragsverarbeitungsvertrag abzuschließen** ist (wobei besonderes Augenmerk auf die vom Auftragsverarbeiter umzusetzenden technischen und organisatorischen Maßnahmen zu legen ist).

Zu beachten ist dabei, dass sämtliche Verpflichtungen des Verantwortlichen zum Schutz von Hinweisgeber*innen auch für den Auftragsverarbeiter gelten (§ 8 Abs 2 letzter Satz HSchG). Dies ist ua deshalb erforderlich, um zu verhindern, dass Verantwortliche über Weisungen an einen Auftragsverarbeiter die **Vertraulichkeitsbestimmungen des HSchG umgehen** können.

PRAXISTIPP

Sollten Auftragsverarbeiter nichtsdestotrotz Weisungen zur Offenlegung der Identität von Hinweisgeber*innen erhalten, ist der Verantwortliche unverzüglich über den Verstoß der Weisung gegen datenschutzrechtliche Bestimmungen zu informieren.[12]

Unternehmen und juristische Personen des öffentlichen Rechts, die nicht Verwaltungsstellen des Bundes sind, können die Aufgaben der internen Stelle auf eine gemeinsame Stelle übertragen (§ 12 Abs 4 HSchG).[13] Bei solchen Kooperationen liegt ex lege eine gemeinsame Verantwortlichkeit iSd Art 4 Z 7 iVm Art 26 DSGVO vor.[14] Die gemeinsame Stelle selbst ist aber internen Stellen gleichgestellt und daher als selbstständige Verantwortliche zu qualifizieren. Diesfalls ist ein sog **Joint Controller Agreement abzuschließen**, in welchem va eine Aufteilung der Verpflichtungen nach der DGSVO vorzunehmen ist (zB Bearbeitung von geltend gemachten Betroffenenrechten). Diese Kooperationsmöglichkeit gilt allerdings unbeschadet der den jeweiligen Organisatio-

[7] Vgl Stellungnahme DSB, 3; www.parlament.gv.at/PtWeb/api/s3serv/file/cb34b15b-dc74-4c93-90fb-b377813afb9b. [8] Außerdem könnten auch nicht unter § 9 Abs 1 VStG fallende Personen erfasst sein, weil § 13 Abs 2 HSchG nur regelt, wer „jedenfalls“ als „Leitung des Unternehmens“ anzusehen ist. [9] In diesem Beitrag werden nur jene Verpflichtungen behandelt, die für die datenschutzkonforme Ausgestaltung eines Hinweisgebersystems besonders relevant sind. [10] Vgl Stellungnahme DSB, 4. [11] Art 16 Abs 1 RL 2019/1937. [12] Dies ist eine inhaltliche Mindestanforderung an Auftragsverarbeitungsverträge gem Art 28 Abs 3 DSGVO. [13] Das HSchG definiert eine solche gemeinsame Stelle – gemeinsam mit *„Dritten, die die Aufgaben der internen Stelle wahrnehmen“* – mit dem Begriff *„mit den Aufgaben der internen Stelle beauftragte Stelle“* (§ 5 Z 8 HSchG). [14] Vgl § 8 Abs 2 HSchG.

nen durch das HSchG auferlegten Verpflichtungen, wie insb jene, die Vertraulichkeit zu wahren, Rückmeldung zu geben und gegen gemeldete Verstöße vorzugehen.

Außerdem bietet § 12 Abs 4 HSchG die Möglichkeit, *„Dritte"* mit sämtlichen Aufgaben der internen Stelle zu *„beauftragen"*. Hierbei stellt sich die Frage, welche **datenschutzrechtliche Rolle den „Dritten"**, die die Aufgaben der internen Stelle wahrnehmen, **zukommt**.[15] Auf Grundlage des Gesetzeswortlauts des HSchG-Entwurfs wäre uE die Einstufung der „Dritten" als Verantwortliche geboten, zumal für interne Stellen ex lege eine Verantwortlichen-Stellung vorgesehen ist (§ 8 Abs 2, 6 HSchG) und die Rechte und Verpflichtungen der interne Stelle *„auch für jede mit den Aufgaben der internen Stelle beauftragte Stelle"*[16] gelten (§ 12 Abs 4 HSchG).

5. Spannungsfeld Datenminimierung, Dokumentationspflichten und Aufbewahrungspflichten

Gem § 8 Abs 8 HSchG sind personenbezogene Daten, die für die Bearbeitung eines Hinweises nicht benötigt werden, nicht zu erheben und unverzüglich (wieder) zu löschen, falls sie unbeabsichtigt erhoben wurden. Dabei handelt es sich um eine spezifische Ausprägung des datenschutzrechtlichen Grundsatzes der Datenminimierung (Art 5 Abs 1 lit c DSGVO), wonach die Verarbeitung personenbezogener Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke notwendige Maß zu beschränken ist. Eine Verletzung der Anforderung in § 8 Abs 8 HSchG kann als **Verletzungen des Datenminimierungs-Prinzips** einen Datenschutzverstoß verwirklichen. Dies kann gem Art 83 Abs 5 DSGVO mit Geldbußen von bis zu 20 Mio Euro oder bis zu 4% des letztjährigen weltweiten Konzernumsatzes sanktioniert werden.

Gleichzeitig ist aber eine **überschießende Löschung von Daten zu vermeiden**, um einerseits angemessene Folgemaßnahmen einleiten und durchführen zu können und andererseits den gesetzlichen Dokumentationspflichten (§ 9 HSchG) sowie der 30-jährigen Aufbewahrungspflicht (§ 8 Abs 9 HSchG) zu entsprechen: *„Personenbezogene Daten sind von einer oder einem Verantwortlichen ab ihrer letztmaligen Verarbeitung oder Übermittlung **dreißig Jahre** und darüber hinaus so lange aufzubewahren, als es für die Durchführung verwaltungsbehördlicher oder gerichtlicher Verfahren oder zum Schutz einer der in Abs 1 Z 1 bis 3 genannten Personen erforderlich und verhältnismäßig ist"* (§ 8 Abs 9 HSchG).

Darüber hinaus müssen Protokolldaten (gem § 9 HSchG) drei Jahre nach Ablauf dieser 30-jährigen Aufbewahrungspflicht aufbewahrt werden (§ 8 Abs 10 HSchG).

HINWEIS

Angesichts des Grundsatzes der Speicherbegrenzung (Art 5 Abs 1 lit e DSGVO) und kritischer Stellungnahmen im Gesetzgebungsverfahren[17] wäre es denkbar, dass diese Aufbewahrungspflichten in der finalen Fassung des HSchG noch verkürzt werden.

Die Einhaltung dieser konträren Pflichten kann durch Festlegung verbindlicher interner Abläufe weitgehend sichergestellt werden, wie etwa durch eine „Whistleblower-Policy". An dieser Stelle sei noch erwähnt, dass bei der Konzeption von Hinweisgebersystem und der diesbezüglichen Abläufe bzw Verantwortlichkeiten die Unabhängigkeit von internen Stellen gewährleistet werden muss (Weisungsfreiheit zur Vermeidung von Interessenkonflikten).[18]

6. Informationsobliegenheiten und Betroffenenrechte

Die Öffnungsklausel Art 23 DSGVO ermöglicht es den MS, unter bestimmten Voraussetzungen **weitreichende Beschränkungen** der Rechte und Pflichten nach Art 12–22 (also auch der Informationspflichten) und Art 34 DSGVO vorzusehen, was in § 8 Abs 7 HSchG erfolgt: Demnach finden die Art 13–18, 21, 34 DSGVO keine Anwendung, solange und insoweit dies zum Schutz der Identität des Hinweisgebers und zur Erreichung der vom HSchG verfolgten Zwecke[19] erforderlich ist.[20]

Unter den vorstehenden Voraussetzungen ist es internen Stellen und der Leitung des Unternehmens auch verboten, *„gegenüber einer von einem Hinweis betroffenen Person Information und Auskunftserteilung zum Hinweis"* zu erteilen (§ 8 Abs 7 HSchG).

Zu beachten ist aber, dass die Betroffenenrechte ab dem Zeitpunkt Anwendung finden, sobald die Beschränkungen zum Schutz der Identität des Hinweisgebers und zur Erreichung der vom HSchG verfolgten Zwecke nicht mehr erforderlich sind. Mangels näherer Bestimmungen zu **Ausmaß und Dauer der Beschränkung** obliegt es den jeweiligen Verantwortlichen, unter Berücksichtigung der Umstände des Einzelfalls, eine Prüfung vorzunehmen. Dieser Umstand wurde vom Bundesministerium für Justiz im Begutachtungsverfahren kritisiert; weiters wurde dazu angemerkt: *„Es sollte diese Beschränkung dementsprechend konkreter und enger ausgestaltet und auch befristet werden"*.[21]

Das HSchG selbst kennt darüber hinaus gewisse Informationspflichten betreffend die Möglichkeit und das Verfahren der Hinweisgebung (§ 10 HSchG). Auf das Verhältnis dieser Informationspflichten zu Art 13, 14 DSGVO wird jedoch nicht eingegangen. Die DSB hat dazu im Begutachtungsverfahren festgehalten, *„dass die Pflicht zur Informationserteilung gem HSchG die Art 13 und 14 unberührt lässt und die Informationen ergänzend bereitzustellen sind"*.[22]

PRAXISTIPP

Die Beschränkungen der Betroffenenrechte gem HSchG sind sowohl in den Datenschutzerklärungen sowie auch in den internen Anweisungen und Prozessen betreffend die Erfüllung der Betroffenenrechte auszuweisen.

7. Datenschutz-Folgenabschätzung

Der Gesetzgeber hat auf Grundlage des HSchG-Entwurfs eine abstrakte Datenschutz-Folgenabschätzung gem ErwGr 92 und Art 35 Abs 10 DSGVO durchgeführt[23] und in den Mat zum HSchG-Entwurf klargestellt, *„dass für einzelne Verarbeitungstätigkeiten aufgrund des HSchG von einer eigenen konkreten Datenschutz-Folgenabschätzung abgesehen werden kann"*.[24] Für die Ein-

[15] Das Justizministerium regte im Begutachtungsverfahren die Klarstellung an, ob „Dritte" in diesem Fall als Auftragsverarbeiter beauftragt werden; vgl Stellungnahme Justizministerium, 6; www.parlament.gv.at/PAKT/VHG/XXVII/SNME/SNME_221188/fname_1462089.pdf. [16] Die Legaldefinition in § 5 Z 8 für *„mit den Aufgaben der internen Stelle beauftragte Stelle"* erfasst ausdrücklich auch *„Dritte, die die Aufgaben der internen Stelle wahrnehmen"*. [17] Der Datenschutzrat bezeichnete die Dauer der Aufbewahrungspflichten im Begutachtungsverfahren als *„grundsätzlich nicht verhältnismäßig"*; vgl Stellungnahme Datenschutzrates, 5; www.parlament.gv.at/PAKT/VHG/XXVII/SNME/SNME_221151/index.shtml [18] Vgl ErwGr 56 RL 2019/1937. [19] Wie insb um Versuche der Verhinderung, Unterlaufung oder Verschleppung von Hinweisen oder Folgemaßnahmen zu unterbinden. [20] Keine Einschränkung erfährt das Recht auf Datenportabilität (gem Art 20), weil dessen Einschränkung zur Erreichung der Ziele des HSchG nicht notwendig ist, zumal ohnehin nur jene Daten davon erfasst wären, welche Betroffene dem Verantwortlichen bereitgestellt haben und die die jeweilige betroffene Person auch selbst betreffen. [21] Vgl Stellungnahme Justizministerium, 4; www.parlament.gv.at/PAKT/VHG/XXVII/SNME/SNME_221188/fname_1462089.pdf [22] Vgl Stellungnahme DSB, 4. [23] www.parlament.gv.at/PAKT/VHG/XXVII/ME/ME_00210/index.shtml. [24] ErläutRV 210 BlgNR 27. GP 9.

führung von Hinweisgebersystemen gem HSchG ist daher **keine Datenschutz-Folgenabschätzung erforderlich**.

8. Exkurs: Meldungen außerhalb des sachlichen Geltungsbereichs des HSchG

Die Beratungspraxis zeigt, dass viele Unternehmen auch für Meldungen von Verstößen außerhalb des sachlichen Anwendungsbereichs des HSchG ein Hinweisgebersystem einrichten möchten. Dabei ist zu beachten, dass die datenschutzrechtlichen Regelungen des HSchG nicht greifen und folglich sämtliche Datenverarbeitungen nach den **allgemeinen datenschutzrechtlichen Vorgaben zu beurteilen** sind.

8.1. Rechtsgrundlage

Als datenschutzrechtliche Grundlage kommt – mangels gesetzlicher Verpflichtung – das berechtigte Interesse des Verantwortlichen (oder eines Dritten) gem Art 6 Abs 1 lit f DSGVO in Betracht. Nach Ansicht der dt Aufsichtsbehörden können die **berechtigten Interessen an der Verhütung/Aufklärung von Betrug und Fehlverhalten** eine geeignete Rechtsgrundlage für Whistleblowing-Datenverarbeitungen darstellen – allerdings geht mit der gebotenen Interessenabwägung im Einzelfall stets eine gewisse Rechtsunsicherheit einher (insb bei Meldung von Verstößen, die nicht gesetzlich verboten sind, sondern nur organisationsintern als unzulässig erachtet werden, zB im internen Code of Conduct).[25]

Für Daten gem Art 10 DSGVO kann § 4 Abs 3 Z 2 DSG als Rechtsgrundlage herangezogen werden. Demnach ist die Verarbeitung solcher Daten ua dann zulässig, wenn *„die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten gem Art 6 Abs 1 lit f DSGVO erforderlich ist, und die Art und Weise, in der die Datenverarbeitung vorgenommen wird, die Wahrung der Interessen der betroffenen Person nach der DSGVO und diesem Bundesgesetz gewährleistet"*.

Wird neben dem verpflichtenden Hinweisgebersystem ein freiwilliges Hinweisgebersystem für sonstige Verstöße eingerichtet, das den Schutzstandards gem §§ 6–13 HSchG entspricht (insb bzgl der Vertraulichkeit der Identitäten), sollte Art 6 Abs 1 lit f DSGVO bzw § 4 Abs 3 Z 2 DSG iVm Art 6 Abs 1 lit f DSGVO in der Regel eine gültige Rechtsgrundlage für die Verarbeitung „normaler" bzw strafrechtlich relevanter Daten darstellen.

Für **Daten gem Art 9 DSGVO** gibt es **keinen Ausnahmetatbestand**, der Datenverarbeitungen aufgrund berechtigter Interessen rechtfertigt. Außerhalb des sachlichen Geltungsbereichs des HSchG wird eine Verarbeitung solcher Daten daher nur in Ausnahmefällen zulässig sein. In Betracht kommen va die Ausnahmetatbestände Art 9 Abs 2 lit b DSGVO (Erforderlichkeit zur Ausübung arbeitsrechtlicher Rechte oder Pflichten; zB bei Hinweis auf sexuelle Belästigung am Arbeitsplatz) und Art 9 Abs 2 lit f DSGVO (Erforderlichkeit zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen).

8.2. Rollenverteilung

Auch die ex lege-Verantwortlichen-Stellung gem § 8 Abs 2 HSchG greift außerhalb des sachlichen Geltungsbereichs des Gesetzes nicht. Deshalb ist die Rollenverteilung nach allgemeinen Grundsätzen zu prüfen. Im Regelfall wird jede Organisation für das von ihr eingerichtete „freiwillige" Hinweisgebersystem verantwortlich sein.

HINWEIS

Organisationen, die sowohl verpflichtende Hinweisgebersysteme gem HSchG als auch „freiwillige" betreiben, könnten mit den Herausforderungen einer divergierenden datenschutzrechtlichen Rollenverteilung konfrontiert sein.

8.3. Informationsobliegenheiten und Betroffenenrechte

Die Information gegenüber Hinweisgeber*innen selbst kann in der Praxis dadurch gewährleistet werden, dass diese vor dem Meldevorgang bestätigen müssen, die angezeigte (oder verlinkte) Datenschutzinformation zur Kenntnis genommen zu haben. Die Information gem Art 14 DSGVO an Personen, die von der Hinweisgebung betroffen sind, gestaltet sich hingegen schwieriger. Damit würde nämlich klargestellt, dass ein Hinweis auf eine (vermeintlich) rechtswidrige Handlung seinerseits/ihrerseits vorliegt, was sowohl die **Aufklärung des Hinweises ernsthaft beeinträchtigen** als auch den Schutz oder die Anonymität des Hinweisgebers gefährden könnte.

Art 14 Abs 5 lit b DSGVO sieht für solche Sonderfälle eine Ausnahmeregelung vor, die greift, wenn die Information *„voraussichtlich die Verwirklichung der Ziele der Verarbeitung unmöglich macht oder ernsthaft beeinträchtigt"*. Ob die Voraussetzungen für eine solche Ausnahme vorliegen (wie insb bei der Gefahr der Zeugenbeeinflussung oder der Vernichtung von Beweismitteln),[26] muss jedoch jeweils **im Einzelfall beurteilt** und entsprechend dokumentiert werden.[27]

PRAXISTIPP

Die Informationspflicht gegenüber den von Hinweisen betroffenen Personen über die sie betreffenden Datenverarbeitungen kann nach Einzelfallbeurteilung entfallen, wenn und solange vernünftigerweise anzunehmen ist, dass eine solche Information die Prüfung einer Meldung ernsthaft beeinträchtigen würde.

Aufklärungshandlungen könnten auch dadurch beeinträchtigt werden, dass anderen Betroffenenrechten entsprochen wird. Das Recht auf Löschung (Art 17 DSGVO) etwa besteht aber nur in den in Abs 1 leg cit genannten Fällen; im gegenständlichen Kontext also va dann, wenn die Daten für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind. Solange solche Datenverarbeitungen daher für die Zwecke der Prüfung/Aufklärung des Hinweises, der Rechtsverfolgung oder zur Erfüllung entsprechender gesetzlicher Aufbewahrungspflichten erfolgen, kann eine Löschung verweigert werden. Anderes gilt beim Recht auf Auskunft (Art 15 DSGVO), das gem Abs 4 leg cit hinsichtlich des Anspruchs auf Kopien (Abs 3 leg cit), nicht aber hinsichtlich des eigentlichen Auskunftsanspruchs (Abs 1 leg cit) beschränkt wird (was allerdings in der Lit bestritten wird).[28] Um Risiken wie Beweismittelverlust oder der Zeugenbeeinflussung hintanzuhalten, könnte es jedoch bereits reichen, die Prüfung von Hinweisen vor Ablauf der einmonatigen Bearbeitungsfrist für Betroffenenrechte (Art 12 Abs 3 DSGVO) vorzunehmen.

[25] *Datenschutzkonferenz*, Orientierungshilfe der Datenschutzaufsichtsbehörden zu Whistleblowing-Hotlines (2018) 5 f; so auch *Feiler/Rieken/Romandy* in *Petsche*, Whistleblowing & Internal Investigations – Praxiskommentar zur Whistleblowing-Richtlinie (2021) 197 f mwN. [26] *Feiler/Rieken/Romandy* in *Petsche*, Whistleblowing, 209. [27] *Bäcker* in *Kühling/Buchner*, DS-GVO – BDSG² (2018) Art 14 Rz 63. [28] *Bäcker* in *Kühling/Buchner*, DS-GVO – BDSG, Art 15 Rz 33; so auch DSB 10. 8. 2020, DSB-D124.339, 2020–0.204.456; aA zB *Specht* in *Sydow*, DSGVO Art 15 Rz 22.

8.4. Aufbewahrung

Umfang und Dauer der Aufbewahrung von personenbezogenen Daten müssen durch den Verantwortlichen selbständig definiert werden. Im Hinblick auf die Grundsätze nach Art 5 DSGVO sind jedenfalls diejenigen personenbezogenen Daten, die für die Prüfung eines Hinweises bzw allfälliger Folgemaßnahmen nicht notwendig sind, gar nicht zu erheben und unverzüglich zu löschen. Der Europäische Datenschutzbeauftragte geht jedenfalls davon aus, dass die zulässige Aufbewahrungsdauer nur zwei Monate ab Abschluss des Verfahrens beträgt.[29]

8.5. Datenschutz-Folgenabschätzung

Verantwortliche haben eine Datenschutz-Folgenabschätzung vor Beginn einer Datenverarbeitung durchzuführen, wenn diese (insb bei Verwendung neuer Technologien) aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hätte (Art 35 Abs 1 DSGVO). Die oben erläuterte Ausnahme (Art 35 Abs 10 DSGVO) ist für „freiwillige" Hinweisgebersysteme – mangels gesetzlicher Verpflichtung – nicht anwendbar.

PRAXISTIPP

Angesichts naheliegender Risiken für die betroffenen Personen wird die vom jeweiligen Verantwortlichen in Selbstverantwortung[30] durchzuführende Schwellenwertanalyse wohl in den meisten Fällen zu dem Schluss kommen müssen, dass eine Datenschutz-Folgenabschätzung erforderlich ist.[31]

Dako 2022/45

[29] EDPS, Guidelines on processing personal information within a whistleblowing procedure (2019) Rz 31 https://edps.europa.eu/sites/edp/files/publication/19-12-17_whisteblowing_guidelines_en.pdf; Datenschutzkonferenz, Orientierungshilfe 11. [30] *Trieb* in *Knyrim*, DatKomm Art 35 DSGVO Rz 8 (Stand 1. 9. 2019, rdb.at). [31] *Pollirer*, Checkliste Whistleblowing, Dako 2020/23, Frage 9.

Zum Thema

Über die Autoren

Dr. Stefan Niederstrasser ist Rechtsanwaltsanwärter bei KPMG Law – Buchberger Ettmayer Rechtsanwälte GmbH und Lehrbeauftragter für Datenschutzrecht an der FH Campus Wien. E-Mail: sniederstrasser@kpmg-law.at

Sebastian Kneidinger ist als Assistant Manager im Bereich Risk Advisory bei KPMG Austria tätig. E-Mail: skneidinger@kpmg.at